

**THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

NANCY BOHNAK and JANET LEA SMITH,

on behalf of themselves and all others
similarly situated,

Plaintiffs,

v.

MARSH & MCLENNAN COMPANIES, INC.,
a Delaware corporation,

and

MARSH & MCLENNAN AGENCY, LLC,
a Delaware limited liability company,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Nancy Bohnak and Janet Lea Smith (“Plaintiffs”) bring this Class Action Complaint against Marsh & McLennan Companies, Inc. and Marsh & McLennan Agency, LLC (individually and collectively, “Defendants”), individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels’ investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard sensitive information of (i) Defendants’ current and former employees and spouses and dependents thereof; (ii) current and former employees of Defendants’ clients, contractors, applicants, and investors; and (iii) individuals whose information Defendants acquired through the purchase of or merger with another business (collectively, “Class Members”).

2. The sensitive information Defendants failed to properly secure, includes, without limitation, name, Social Security or other federal tax identification number, driver’s license or

other government issued identification, and passport information (collectively, “personally identifiable information” or “PII”).

3. According to its website, Defendant Marsh and McLennan Companies, Inc. (“MMC”) “is the world’s leading professional services firm in the areas of risk, strategy and people.”¹ It is a Fortune 250 company with “Clients in more than 130 Countries,” “76,000 Global Colleagues,” and “Average Revenue of \$17 billion.”²

4. Defendant Marsh & McLennan Agency, LLC (“MMA”) “is a wholly owned subsidiary of [MMC], serving the risk prevention and insurance needs of middle market companies in the United States.”³

5. On or before April 26, 2021, Defendants learned that “an unauthorized actor had leveraged a vulnerability in a third party’s software since at least April 22, to gain access to a limited set of data in its environment” (the “Data Breach”).⁴

6. The Data Breach ended on April 30, 2021, approximately one week after it commenced.

7. At the time of the Data Breach, the compromised set of data stored the PII of at least 7,000 individuals.

8. At the time of the Data Breach, the compromised set of data included Social Security or other federal tax identification numbers, driver’s license or other government issued identification, and passport information that were not encrypted.

¹ See <https://www.mmc.com/> (last visited July 14, 2021).

² See <https://careers.mmc.com/global/en> (last visited July 14, 2021).

³ See <https://www.marshmma.com/about> (last visited July 14, 2021).

⁴ Ex. 1 (Letter and sample *Notice of Data Breach* filed with New Hampshire Attorney General).

9. On or around June 30, 2021, Defendants began notifying various states Attorneys General and Plaintiffs and Class Members of the Data Breach.⁵

10. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII exposed to “unauthorized activity” included name, Social Security or other federal tax identification number, driver’s license or other government issued identification, and passport information.

11. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

12. This PII was compromised due to Defendants’ negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. In addition to Defendants’ failure to prevent the Data Breach, after discovering the breach, Defendants waited approximately two months to report it to various states’ Attorneys General and Class Members. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

13. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

⁵ *Id.*

14. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

15. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII.

16. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be

entitled to injunctive and other equitable relief.

II. PARTIES

17. Plaintiff Nancy Bohnak (“Bohnak”) is a Citizen of Florida residing in Orange County, Florida. Mrs. Bohnak received Defendants’ *Notice of Data Breach*, dated June 30, 2021, on or about that date.⁶ The notice stated that an unauthorized actor gained access to Mrs. Bohnak’s Social Security number or other federal tax identification number.⁷

18. Plaintiff Janet Lea Smith (“Smith”) is a Citizen of Florida residing in Volusia County, Florida. Ms. Smith received Defendants’ *Notice of Data Breach*, dated June 30, 2021, on or about that date.⁸ The notice stated that an unauthorized actor gained access to Ms. Smith’s Social Security number or other federal tax identification number.⁹

19. Defendant Marsh & McLennan Companies, Inc. is a corporation organized under the laws of Delaware, headquartered at 1166 Avenue of the Americas, New York, New York, with its principal place of business in New York, New York.

20. Defendant Marsh & McLennan Agency, LLC is a limited liability company organized under the laws of Delaware, headquartered at 1166 Avenue of the Americas, New York, New York, with its principal place of business in New York, New York.

21. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently

⁶ Ex. 2 (*Notice of Data Breach* sent to Mrs. Bohnak).

⁷ *Id.*

⁸ Ex. 3 (*Notice of Data Breach* sent to Mrs. Smith).

⁹ *Id.*

unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

22. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

23. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendants to establish minimal diversity.

24. The Southern District of New York has personal jurisdiction over Defendants named in this action because Defendants and/or their parents or affiliates are headquartered in this District and Defendants conduct substantial business in New York and this District through their headquarters, offices, parents, and affiliates.

25. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants and/or their parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

26. Defendants provides professional services in the areas of risk, strategy, and people.

27. Plaintiffs and Class Members entrusted Defendants, or companies that Defendants purchased or merged with, with sensitive and confidential information, including name, Social Security or other federal tax identification number, driver's license or other government issued

identification, and passport information, which include information that is static, does not change, and can be used to commit myriad financial crimes.

28. Plaintiffs and Class Members relied on these sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

29. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

30. On or about June 30, 2021, Defendants sent Plaintiffs and other Class Members a *Notice of Data Breach*.¹⁰ Defendants informed Plaintiffs and other Class Members that:

WHAT HAPPENED. On April 26, 2021, we discovered that an unauthorized actor had leveraged a vulnerability in a third party's software since at least April 22, to gain access to a limited set of data in our environment. As soon as we became aware of the issue, we launched an investigation and took measures to restrict any further unauthorized activity or access to data; that access ended on April 30.

WHAT INFORMATION WAS INVOLVED.

We have determined that the personal information involved in this incident included your name and the following: Social Security or other federal tax id number.

WHY DO WE HAVE YOUR DATA. We held this information because you are a current or former colleague, spouse or dependent of a colleague, employee or former employee of a client, contractor, applicant, investor, or because we or one of our businesses purchased or merged with a business with whom you had such a relationship.

WHAT WE ARE DOING. We notified law enforcement and took

¹⁰ Ex. 2 (*Notice of Data Breach* sent to Mrs. Bohnak).

immediate actions to terminate the unauthorized actor's access and prevent future access. These measures included resetting IT administrator access rights, and imposing additional restrictions on access to various systems on our network.¹¹

31. On or about June 30, 2021, Defendants notified various state Attorneys General, including New Hampshire's Attorney General, of the Data Breach. Defendants also provided the Attorneys General with letters and/or "sample" notices of the Data Breach that reaffirm "the personal information involved in this incident included the name and Social Security or other federal tax identification number, driver's license or other government issued identification, and passport information" of Class Members.¹²

32. Defendants admitted in the *Notice of Data Breach*, the letters to the Attorneys General, and the "sample" notices of the Data Breach that unauthorized third persons accessed files that contained sensitive information about Plaintiffs and Class Members, including name, Social Security or other federal tax identification number, driver's license or other government issued identification, and passport information.

33. In response to the Data Breach, Defendants claims that they "took immediate actions to terminate the unauthorized actor's access and prevent future access. These measures included resetting IT administrator access rights, and imposing additional restrictions on access to various systems on our network."¹³ However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

¹¹ *Id.*

¹² Ex. 1 at 1.

¹³ Exs. 1, 2.

34. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

35. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for more than 7,000 individuals.

Defendants Acquire, Collect, and Store the PII of Plaintiffs and Class Members.

36. Defendants acquired, collected, and stored the PII of Plaintiffs and Class Members at least from 2014 to 2021.

37. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

38. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

39. Defendants could have prevented this Data Breach by properly securing and encrypting the set of data in their environment containing the PII of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data, especially decade-old data from former employees and their dependents and spouses; former employees of Defendants' clients, contractors, applicants, and investors; or individuals no longer affiliated with businesses that

Defendants purchased or merged with.

40. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

41. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

42. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁴ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."¹⁵

43. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

44. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,

¹⁴ 17 C.F.R. § 248.201 (2013).

¹⁵ *Id.*

and bank details have a price range of \$50 to \$200.¹⁶ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁷ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁸

45. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹⁹

46. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

¹⁶ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited July 14, 2021).

¹⁷ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited July 14, 2021).

¹⁸ *In the Dark*, VPNOOverview, 2019, available at: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed July 14, 2021).

¹⁹ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited July 14, 2021).

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

47. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²⁰

48. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change— Social Security number or other federal tax identification number, driver’s license or other government issued identification, and passport information.

49. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²¹

50. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

²⁰ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last accessed July 14, 2021).

²¹ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed July 14, 2021).

51. The fraudulent activity resulting from the Data Breach may not come to light for years.

52. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²²

53. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants’ data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

54. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

55. Defendants were, or should have been, fully aware of the unique type and the significant volume of data in the set of data in Defendants’ environment, amounting to potentially tens or hundreds of thousands of individuals’ detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

56. To date, Defendants have offered Plaintiffs and Class Members only two years of

²² *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed July 14, 2021).

credit monitoring and identity theft detection and resolution services through a single credit bureau, Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

57. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Plaintiff Nancy Bohnak's Experience

58. In or around 2014, Mrs. Bohnak's employment with Defendant MMA ended. As a condition of Mrs. Bohnak's employment, Defendants required that she entrust her PII, including but not limited to her Social Security or other federal tax id number, which Defendants acquired directly from Mrs. Bohnak or through their purchase of or merger with Mrs. Bohnak's prior employer.

59. Mrs. Bohnak received the Notice of Data Breach, dated June 30, 2021, on or about that date.

60. As a result of the Data Breach notice, Mrs. Bohnak spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

61. Additionally, Mrs. Bohnak is very careful about sharing her PII. She has never knowingly transmitted her unencrypted sensitive PII over the internet or any other unsecured source.

62. Mrs. Bohnak stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for

her various online accounts.

63. Mrs. Bohnak suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Mrs. Bohnak entrusted to Defendants for the purpose of her employment, which was compromised in and as a result of the Data Breach.

64. Mrs. Bohnak suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

65. Mrs. Bohnak has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security or other federal tax id number being placed in the hands of unauthorized third parties and possibly criminals.

66. Mrs. Bohnak has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Janet Lea Smith's Experience

67. In or around 2016, Mrs. Smith's employment with Defendant MMA ended. As a condition of Mrs. Smith's employment, Defendants required that she entrust her PII, including but not limited to her Social Security or other federal tax id number, which Defendants acquired directly from Ms. Smith or through their purchase of or merger with Ms. Smith's prior employer.

68. Ms. Smith received the Notice of Data Breach, dated June 30, 2021, on or about that date.

69. As a result of the Data Breach notice, Ms. Smith spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-

monitoring her accounts. This time has been lost forever and cannot be recaptured.

70. Additionally, Ms. Smith is very careful about sharing her PII. She has never knowingly transmitted her unencrypted sensitive PII over the internet or any other unsecured source.

71. Ms. Smith stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

72. Ms. Smith suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Smith entrusted to Defendants for the purpose of her employment, which was compromised in and as a result of the Data Breach.

73. Ms. Smith suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

74. Ms. Smith has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security or other federal tax id number being placed in the hands of unauthorized third parties and possibly criminals.

75. Ms. Smith has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

76. Plaintiffs bring this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

77. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All individuals whose PII was compromised in the breach that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around June 30, 2021 (the “Nationwide Class”).

78. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows:

All current and former employees of Defendants, or any of their direct or indirect subsidiaries, who had contracts related to PII that was compromised in the breach that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around June 30, 2021 (the “Employees Class”).

79. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants’ parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

80. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

81. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the “Class”) are so numerous that joinder of all members is impracticable. Defendants have identified thousands of individuals whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants’ records. Defendants advised the Iowa Attorney General that the Data Breach affected 7,208 Iowa residents, and the Data Breach affected individuals in other states, including Florida (where Plaintiffs reside) and California, Indiana, and

New Hampshire (where Defendants filed notices of the Data Breach with the Attorneys General).

82. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;
- b. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendants had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;
- e. Whether and when Defendants actually learned of the Data Breach;
- f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;
- h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to

safeguard the PII of Plaintiffs and Class Members;

- k. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;
- l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and
- m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

83. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

84. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

85. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action

vigorously.

86. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

87. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

88. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

89. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

90. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

91. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

92. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendants on the one hand, and

- Plaintiffs and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendants breached the implied contract;
 - f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;
 - g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
 - h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,
 - i. Whether Class Members are entitled to actual damages, statutory damages, nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

93. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

94. As a condition of (i) employment with Defendants, (ii) employment with Defendants' clients, contractors, applicants, and investors or its subsidiary, and/or (iii) relationships with businesses that Defendants purchased or merged with, Plaintiffs and Class Members entrusted their PII, including name, Social Security or other federal tax identification number, driver's license or other government issued identification, and/or passport information.

95. Plaintiffs and the Nationwide Class entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for

business purposes only, and/or not disclose their PII to unauthorized third parties.

96. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

97. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

98. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendants' possession was adequately secured and protected.

99. Defendants also had a duty to exercise appropriate clearinghouse practices to remove the PII of Plaintiffs and Class Members it was no longer required to retain pursuant to regulations.

100. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

101. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Defendants with their confidential PII, a necessary part of treatment from or employment with Defendants or its subsidiary.

102. Defendants were subject to an “independent duty,” untethered to any contract between Defendants and Plaintiffs or the Nationwide Class.

103. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants’ inadequate security practices.

104. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants’ systems.

105. Defendants’ own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendants’ misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants’ misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendants.

106. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendants’ possession.

107. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

108. Defendants had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendants’ possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such

notice was necessary to allow Plaintiffs and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

109. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

110. Defendants have admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

111. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendants' possession or control.

112. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

114. Defendants, through their actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII.

115. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove the PII of Plaintiffs and the Nationwide Class they were no longer required to retain pursuant to regulations.

116. Defendants, through their actions and/or omissions, unlawfully breached their duty

to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

117. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

118. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

119. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

120. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Nationwide Class.

121. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

122. Plaintiffs and the Nationwide Class are within the class of persons that the FTC Act

was intended to protect.

123. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Nationwide Class.

124. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

125. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury

and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

126. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

127. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Employees Class)

128. Plaintiffs and the Employees Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

129. Defendants required Plaintiffs and the Employees Class to entrust their PII, including name, Social Security or other federal tax identification number, driver's license or other government issued identification, and/or passport information, as a condition of their employment.

130. As a condition of their employment with Defendant MMA, Plaintiffs and the Employees Class entrusted their PII to Defendants. In so doing, Plaintiffs and the Employees Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Employees Class if their data had been breached and compromised or stolen.

131. Plaintiffs and the Employees Class fully performed their obligations under the implied contracts with Defendants.

132. Defendants breached the implied contracts they made with Plaintiffs and the Employees Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

133. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and the Employees Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

134. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and the Employees Class are entitled to and demand actual, consequential, and nominal damages.

COUNT III
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class)

135. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

136. At all times during Plaintiffs' and the Nationwide Class's interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiffs' and the Nationwide Class's PII that Plaintiffs and the Nationwide Class entrusted to Defendants.

137. As alleged herein and above, Defendants' relationship with Plaintiffs and the Nationwide Class was governed by terms and expectations that Plaintiffs' and the Nationwide Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

138. Plaintiffs and the Nationwide Class entrusted Plaintiffs' and the Nationwide Class's PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized third parties.

139. Plaintiffs and the Nationwide Class also provided Plaintiffs' and the Nationwide Class's PII to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that PII from unauthorized disclosure.

140. Defendants voluntarily received in confidence Plaintiffs' and the Nationwide Class's PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

141. Due to Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiffs and the Nationwide Class's PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Nationwide Class's confidence, and without their express permission.

142. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiffs and the Nationwide Class have suffered damages.

143. But for Defendants' disclosure of Plaintiffs' and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Nationwide Class's PII as well as the resulting damages.

144. The injury and harm Plaintiffs and the Nationwide Class suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and the Nationwide Class's PII. Defendants knew or should have known their methods of accepting and securing Plaintiffs' and the Nationwide Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Nationwide Class's PII.

145. As a direct and proximate result of Defendants' breach of their confidence with Plaintiffs and the Nationwide Class, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the

impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

146. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

147. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendants and that the Court grant the following:

- A. For an Order certifying the Nationwide Class and the Employees Class and appointing Plaintiffs and their Counsel to represent each such Class;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendants to protect, including through encryption, all data collected

through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

- iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
- iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
- v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;
- vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

- x. requiring Defendants to conduct regular database scanning and securing checks;
- xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
- xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendants to meaningfully educate all Class Members about the

threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

- xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL


Plaintiffs hereby demand that this matter be tried before a jury.

Date: New York, New York
July 15, 2021

Respectfully Submitted,

MORGAN & MORGAN, P.A.
Attorneys for Plaintiffs and Proposed Class

By: _____


Amanda Peterson, Esq. (AP1797)
90 Broad Street, Suite 1011

New York, New York 10004
(212) 564-4568
apeterson@forthepeople.com

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN
COMPLEX BUSINESS
DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@forthepeople.com
rmaxey@forthepeople.com
**pro hac vice* to be filed